International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

SURVEY OF HIGHLY SECURED METHODS FOR IMAGE TRANSMISSION USING IMAGE SEGMENTATION, PERMUTATION AND MULTI ENCRYPTION TECHNIQUE

Pratibha Pradhan[1], Rasmiranjan Samantray[2]

[1,2]Central College of Engineering and Management, Kabir Nagar, Raipur, Chhattisgarh Swami Vivekanand Technical University, Raipur, Chhattisgarh, India

---

Abstract - In recent years, several encryption schemes have been proposed to protect data from unauthorized access. It is not suitable to use traditional encryption algorithms for image encryption which were proposed for textual data. The encryption schemes used for images are computationally expensive and power hungry, hence not suitable for mobile phone devices. The protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption. There are so many different techniques are used to protect confidential image data from an unauthorized access.

Keywords: Encryption, Decryption, Segmentation, Key.

INTRODUCTION:

With the advent of technological development multimedia transfer is growing every day. Mobile phones are the major way of transferring multimedia data these days. One of the most debatable critical issues of this age is the prevention of illegal access and sharing of multimedia data particularly the images, as digital images carry a large amount of information. This security issue has attracted the attention of many researchers in last two decades. There are different ways to secure data which include encryption and water marking [1]. Encryption is done by converting data into such a form that it cannot be read by unauthorized user. The protection of this multimedia data can be done with encryption. Encryption has long been used by militaries and governments to facilitate secret communication. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but to unauthorized users.

Encryption:

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an Encryption algorithm – a cipher – generating cipher text that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required.

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, ecommerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years [2]. Data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by unauthorized users.

LITERATURE SURVEY

Entire idea behind the proposed algorithm is built upon scrambling of image pixels based on random number generators. Authors in [3] presented similar work on image the Authors in [4] have mentioned the positive consequences of using a shuffle based technique. The proposed algorithm design also considered the author in [5] mentioning the downside of using linear congruently generator as the PRNG which includes statistical determinism due to the mechanical nature of the algorithm. Authors in [6] have talked about using linear congruential generator of order k>1 to generate random numbers which mimics true random generators. Authors in [7] presented an image encryption technique based on shuffling of pixel blocks with the help of chaotic map which predicts pixel positions. In this paper we propose a shuffle algorithm with minimal compression issues,

loss of data and also an undemanding encryption and decryption of image files.

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding.

Images are different from texts in many aspects such as high correlation among pixels and high redundancy. Thus, a variety of new image encryption schemes have been proposed [8]. Although we may use the traditional encryption algorithms to encrypt images directly, it is not a good idea for two reasons. The first is the image size is often larger than text. Consequently, the traditional encryption algorithms need longer time to directly encrypt the image data, the second, is the decrypted text must be equal to the original text, but this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable. According to image encryption techniques try to convert an image to another one that is hard to understand. On the other side, image decryption retrieves the original image from the encrypted one. Most of these proposed algorithms concentrate on dividing the image into different blocks which result in a stronger encryption algorithm with less correlation between the shares [9].

PROPOSED METHODOLOGY:

Pixel- Shuffling:

This section entails the core idea of the working algorithm. The image encryption methodology adapted in the algorithm majorly depends on shuffling the pixels according to the random numbers that are generated using the techniques covered in the previous sections. The basic operation in shuffling involves swapping two pixels to remove them from their original position. This process is repeated multiple times, in row & column order to have maximum displacement for each pixel.

a) Row Shuffle

The initial step of the algorithm after pseudo random number generation is to shuffle the pixels. This process starts with the row having the zero index being exchanged with the row number that is in the zeroth index of the random number array. Hence in our case the zeroth row gets exchanged with the third row and the current state of the image is saved. Now, the row pointer moves to the second row (or the first row index) and the corresponding random row number is taken from the random array i.e. the second row is exchanged with the first row and the state of the matrix is saved again.

(b) Column Shuffle

Similar procedure is followed again but this time, the columns of the pixel matrix are shuffled instead of the rows. This leads to the interchanging of the columns in a fashion that is predicted by the random numbers generated earlier. Our aim to have a column shuffle accompanying the row order shuffle is to displace the pixels in column order also rather than just in row order ensuring maximum diffusion. After both the row and the column shuffle are done, the algorithm returns a randomly shuffled array that has been subjected to a row wise shuffle and a column wise shuffle at the same time.

Encryption Process:

The encryption block starts by determining the number of iterations, which defines the number of times whole algorithm is repeated to get good results. Initially the counter is initialized at 0 and then it can be increased by one count after each iteration so that image is visually not in a condition to get recognized and shows robustness against cryptographic attacks. The proposed image encryption scheme shows comparable results and robustness against attacks with one iteration only, which in turn reduces the power consumption of the algorithm. To start shuffling of pixels in the rows, sum of all elements in rows is computed to get a row vector of 1 × 256. Then Modulo-2 of this sum is computed to convert the data in the form of binary numbers. Then shuffling of pixels is performed by using obtained Modulo-2 vector sum by right circular shifting pixels at 0s positions and left circular shifting of pixels at 1s positions. All the pixels in rows are shuffled using this operation. To start shuffling of pixels in the columns of already row shuffled image, sum of all elements in columns is computed to get a vector of 1×256.ThenModulo-2of this summited computed to convert the data in the form of 0s and 1s.
Decryption Process:

Number of maximum iterations is denoted which can be increased by counter of one. ITERmax is kept same in encryption and decryption blocks of algorithm to repeat the steps same time in both blocks. Column key vector (Kc) used to apply zeta function on rows of the final scrambled image, then row key vector (Kr) is used to apply zeta function on the columns. Sum of all elements in columns is computed to get a vector of 1×256. Then Modulo-2 of this sum is computed to convert the data in the form of 0s and 1s. Then shuffling of obtained Modulo-2 vector sum is performed by up circular shifting of pixels positioned at 0s and down circular shifting of 1s positions. Sum of all elements in rows is computed to get a vector of 1×256. Then Modulo-2 of this sum is computed to convert the data in the form of 0s and 1s. Then shuffling of obtained Modulo-2 vector sum is performed by right circular shifting of pixels on

positions of 0s and left circular shifting those at 1s positions.

Permutation Process:

In this process we are changing the original sequence of image parts. This process will increase the security during transmission. In mathematics, the notion of permutation relates to the act of arranging all the members of a set into some sequence or order, or if the set is already ordered, rearranging its elements, a process called permuting. These differ from combinations, which are selections of some members of a set where order is disregarded. Permutations are studied in almost every branch of mathematics. They are also appearing in many other fields of science. In computer science they are used for analysing sorting algorithms, in quantum physics for describing states of particles and in biology for describing RNA sequences. Permutation can be defined as bisections from a set onto itself. All permutations of a set with n elements from a symmetric group denoted Sn, where the group operation is function composition.

RESULT ANALYSIS:

In this section, we present the experimental results to exemplify the efficiency and performance of the proposed encryption algorithm. The complete reverse algorithm has also been tested to ensure uniformity between the source image and the decrypted image. The result from **permutation based image encryption algorithm using block cipher approach 2015** is shown below-

SENSITIVITY VALUES FOR THE TESTED IMAGES

Example	NPCR	UACI
A	0.9957	0.1483
B	0.9929	0.2224
C	0.9952	0.1454

Than permutation based image encryption algorithm using block cipher approach 2015 result is implemented by **Energy Efficient Image Encryption Algorithm** in 2017 and the given result is as shown below –

NPCR AND UACI OF ENCRYPTED IMAGES

Image Name	NPCR	UACI
Cameraman	99.5956	33.5811
Lena	99.5859	33.4201
Checkerboard	99.6201	33.7082
Football	99.6078	33.6101
Rice	99.7120	33.7791

CONCLUSION:

In this paper we proposed an image encryption algorithm based on seed values acquired from multiple pseudo random number generators which were comprehensible and had a straight forward implementation. The presented technique provides high security and confidentiality in transmission of image data over networks or storage of the same. The encryption method in our work has been tested on different image formats with best possible seed values and packs immense flexibility due to variable number of parameters that can be used as a deciding factor for the encryption process. The algorithm performs the operation in linear time, much faster than the existing image encryption techniques. The approach used is a simple, efficient and yet effective way to achieve image encryption using pre-existing technology. It is easy to comprehend and can be translated into techniques to implement image encryption on handheld devices or as a module. which could be integrated into a bigger system.

REFERENCES:

[1] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on rubik's cube principle," Journal of Electrical and Computer Engineering, vol. 2012, p. 7, 2012.

[2] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," Optics and Lasers in Engineering, vol. 88, pp. 197–213, 2017.

[3] X. Chai, "An image encryption algorithm based on bit level brownian motion and new chaotic systems," Multimedia Tools and Applications, vol. 76, no. 1, pp. 1159–1175, 2017.

[4] W. Wang, H. Tan, Y. Pang, Z. Li, P. Ran, and J. Wu, "A novel encryption algorithm based on dwt and multichaos mapping," Journal of Sensors, vol. 2016, 2016.

[5] G. Ye, H. Zhao, and H. Chai, "Chaotic image encryption algorithm using wave-line permutation and block diffusion," Nonlinear Dynamics, vol. 83, no. 4, pp. 2067–2077, 2016.

[6] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using dna and chaotic logistic maps," Multimedia Tools and Applications, vol. 75, no. 10, pp. 5455–5472, 2016. [7] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic s-boxes composed of dna sequences," Multimedia Tools and Applications, vol. 75, no. 8, pp. 4363–4382, 2016.

Author Profile

Pratibha Pradhan received the B.E degree in Electronics and Telecommunication Engineering from the Chhattisgarh Swami Vivekananda Technical University (CSVTU), Bhilai, India, in 2017, and pursuing her M.Tech.

Degree in Digital Electronics in CSVTU, Bhilai, India. Her research interests include cryptography, Image Processing.

Rasmiranjan Samantray is Assistant Professor in CCEM Raipur, India. He is a BE in Electronics and Telecommunication Engineering, M.Tech. in Communication System Engineering From KIIT University Bhubaneswar.